



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/665,386	09/18/2003	Radia J. Perlman	SUN06-38(P9238)	4209
58408	7590	07/18/2007	EXAMINER	
BARRY W. CHAPIN, ESQ. CHAPIN INTELLECTUAL PROPERTY LAW, LLC WESTBOROUGH OFFICE PARK 1700 WEST PARK DRIVE WESTBOROUGH, MA 01581			DADA, BEEMNET W	
ART UNIT		PAPER NUMBER		
2135				
MAIL DATE		DELIVERY MODE		
07/18/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/665,386	PERLMAN, RADIA J.	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 17 April 2007.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-44 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-44 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is in reply to an amendment filed on April 17, 2007. Claims 1-44 are pending.

Response to Arguments

2. Applicant's arguments with respect to claims 1-44 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 44 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claim 44 recites the limitation "said ephemizer" in line 4 of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-44 are rejected under 35 U.S.C. 102(b) as being anticipated by Perlman US 6,363,480 B1.

8. As per claims 1, 42, 43 and 44, Perlman teaches a method for performing blinded ephemeral decryption of a message, the method comprising the steps of:

receiving from a first node at an ephemerizer an ephemeral key ID and a message blinded and encrypted with an ephemeral encryption key of an ephemeral key pair to form a blinded and encrypted message (i.e., doubly encrypted symmetric key), said ephemeral key pair associated with said ephemeral key ID (i.e., receiving at an ephemeizer, a symmetric key encrypted with an encryption key of party B (i.e., blinded), and encrypted by ephermeral encryption key, column 8, lines 18-31, also note that ephemeral message format includes ephemral key identifier, column 7, lines 23-42);

decrypting said blinded and encrypted message using an ephemeral decryption key of said ephemeral key pair to form a blinded message (i.e., decrypting the doubly encrypted symmetric key using ephermeral key to form symmetric key encrypted with party B's key, column 8, lines 22-9);

communicating said blinded message to said first node (i.e., passing the encrypted symmetric key, column 8, lines 28-31); and

irretrievably deleting said ephemeral decryption key in response to a specified event [column 8, lines 37-39].

9. As per claim 19, Perlman teaches a method for performing blind ephemeral decryption of a message M that has been encrypted to form an encrypted message, comprising the steps of:

in a first blinding step, blinding said encrypted message at a first node with a blinding function z (i.e., encryption/decryption function) to form a first blinded and encrypted message, wherein z has an inverse z^{-1} (i.e., encrypting a symmetric key using an encryption key of Party B and then doubly encrypting the symmetric key using ephemeral encryption key, column 8, lines 12-15);

in a first communicating step, communicating said first blinded and encrypted message from said first node to a decryption agent (i.e., Party B forwarding the doubly encrypted symmetric key to an ephermerizer, column 8, lines 19-21);

decrypting said first blinded and encrypted message by said decryption agent using an ephemeral decryption function to form a first blinded message, wherein said ephemeral decryption function is the inverse of said ephemeral encryption function (i.e., decrypting the symmetric key using ephemeral key, column 8, lines 22-26);

in a second communicating step, communicating said first blinded message from said decryption agent to said first node(i.e., passing the encrypted symmetric key, column 8, lines 28-31); and

in a first unblinding step, unblinding said first blinded message using z^{-1} , to obtain said message M (i.e., Party B decrypting the encrypted symmetric key using its own key, column 8, lines 28-31); and

irretrievably deleting said ephemeral decryption key in response to a specified event [column 8, lines 37-39].

10. As per claims 2-4, Perlman further teaches the system wherein said ephemeral key ID is associated with an ephemeral RSA public and private key pair / Diffe-Hellman key pair /

symmetric key pair, corresponding to said ephemeral encryption key and said ephemeral decryption key, respectively [column 5, lines 10-21].

11. As per claims 5-16, Perlman further teaches the system further including prior to the receiving step, the step of generating said ephemeral key ID and said ephemeral encryption and decryption keys of said ephemeral key pair [column 7, lines 22-36 and column 5, lines 9-24].
12. As per claims 17 and 18, Perlman further teaches the method wherein said specified event is the recognition of a predetermined date and time / in response to a request by a user to delete said ephermal decryption key [column 5, lines 24-25 and column 8, lines 37-39].
13. As per claims 20 and 21, Perlman further teaches the method wherein said first node and said decryption agent are communicably coupled via a network, and at least one of said first and second communicating steps comprises the step of communicating the respective message over said network [figure 4].
14. As per claim 22, Perlman further teaches the method wherein said first communicating step comprises the step of communicating said first blinded and encrypted message from said first node to said decryption agent via an anonymizer node and said second communicating step comprises the step of communicating said first blinded message from said decryption agent to said first node via said anonymizer node [column 8, lines 19-31].

15. As per claims 23, 40, and 41, Perlman further teaches the method further including the step of rendering said ephemeral decryption function irretrievably deleted upon the occurrence of said specified event [column 5, lines 24-25 and column 8, lines 37-39].

16. As per claim 24, Perlman further teaches the method further including the step of generating said message at said first node [column 8, lines 18-31].

17. As per claims 25-30, Perlman further teaches the method wherein said ephemeral encryption and decryption functions are respectively, ephemeral public and private keys of an ephemeral public key pair [column 5, lines 10-22].

18. As per claims 31-34, Perlman further teaches the method further comprising the steps of: obtaining an ephemeral public key associated with said decryption agent, wherein said ephemeral public key is a Diffie-Hellman public key of the form $g^{sup.x} \text{ mod } p$, selecting a blinding number y having an inverse blinding number $y^{sup.-1}$ that satisfies $y^*y^{sup.-1} = 1 \text{ mod } p-1$, raising said public key $g^{sup.x} \text{ mod } p$ to the power y to obtain $g^{sup.xy} \text{ mod } p$, raising g to the power y to form $g^{sup.y} \text{ mod } p$, encrypting said message M using $g^{sup.xy} \text{ mod } p$ to form an encrypted message of the form $[M]g^{sup.xy} \text{ mod } p$, storing a copy of said encrypted message $[M]g^{sup.xy} \text{ mod } p$, and storing a copy of $g^{sup.y} \text{ mod } p$ (i.e., encryption using RSA by public/private key pairs, which is inherently implied in Perlman, column 5, lines 10-19).

19. As per claims 35-39, Perlman further teaches the method including, prior to said first blinding step, the steps of: selecting a blinding number y having an inverse blinding number $y^{sup.-1}$; in a second blinding step, blinding said message M using said blinding number y to

form a second blinded message; forwarding said second blinded message to an encryption agent; encrypting by said encryption agent said second blinded message to form a second blinded and encrypted message, wherein said ephemeral encryption is performed using said ephemeral encryption function and wherein said ephemeral encryption function and said corresponding ephemeral decryption function are secret symmetric ephemeral encryption and ephemeral decryption keys, respectively; forwarding said second blinded and encrypted message from said encryption agent to said first node; and in a second unblinding step, unblinding said second blinded and encrypted message using said inverse blinding number y.sup.-1 to form said encrypted message [column 8, lines 19-38].

Conclusion

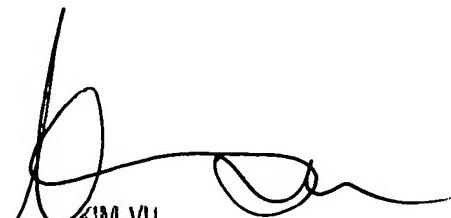
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet W Dada

July 7, 2007



KIM VU
SUPERVISION PATENT EXAMINER
TECHNOLOGY CENTER 2100